Goppa codes

13^{th} January 2006

1. Let

$$G = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{pmatrix}$$

be a generator matrix for the generalised RS code $GRS_k(\alpha, \mathbf{v})$. Let C be the code with generator matrix $\left(G|\mathbf{u}^T\right)$, where $\mathbf{u} = (0, \ldots, 0, u)$, for some $u \in \mathbf{F}_q^*$. Let $\mathbf{v}' = (v_1', \ldots, v_n')$ be such that $GRS_{n-k}(\alpha, \mathbf{v}')$ is the dual of $GRS_k(\alpha, \mathbf{v})$.

i. Show that there is some $w \in \mathbf{F}_q^*$ such that

$$\sum_{i=1}^{n} v_i v_i' \alpha_i^{n-1} + uw = 0$$

ii. Show that

$$H' = \begin{pmatrix} v_1' & v_2' & \cdots & v_n' & 0 \\ v_1'\alpha_1 & v_2'\alpha_2 & \cdots & v_n'\alpha_n & 0 \\ v_1'\alpha_1^2 & v_2'\alpha_2^2 & \cdots & v_n'\alpha_n^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_1'\alpha_1^{n-k} & v_2'\alpha_2^{n-k} & \cdots & v_n'\alpha_n^{n-k} & w \end{pmatrix}$$

is a parity-check matrix for C.

iii. Prove that C is an MDS code.

2. Let n be odd and let $\mathbf{F}_{2^m}$ be an extension of $\mathbf{F}_2$ containing all the n^{th} roots of 1. Let α be a primitive n^{th} root of 1 in $\mathbf{F}_{2^m}$ and let $L = \left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$. For $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathbf{F}_2^n$, let

$$R_c(z) = \sum_{i=0}^{n-1} c_i x^i$$

and let $\hat{c}(z)$ be its Mattson-Solomon polynomial.

i. Show that $\hat{c}(z) = (z\,(z^n+1)\,R_c(z)\,(\operatorname{mod} z^n - 1))$ and

$$R_c(z) = \sum_{i=0}^{n-1} \frac{\hat{c}\left(\alpha^i\right)}{z + \alpha^i}$$

ii. Show that the Goppa code $\Gamma(L, g)$ is equal to

$$\Gamma(L, g) = \left\{\mathbf{c} \in \mathbf{F}_2^n : \left(z^{n-1}\hat{c}(z)\,(\operatorname{mod} z^n - 1)\right) \cong 0 (\operatorname{mod} g(z))\right\}$$

Hint: For (i), show that $z\,(z^n+1)\,R_c(z) = \sum_{i=0}^{n-1} c_i z \prod_{j \neq i}\left(z + \alpha^j\right)$. Then show that $\left(z \prod_{j\neq i}\left(z+\alpha^j\right)(\operatorname{mod} z^n - 1)\right) = \sum_{j=0}^{n-1} \alpha^{-ij} z^j$ by multiplying both sides by $z + \alpha^i$. For (ii), show that $\mathbf{c} \in \Gamma(L, g)$ if and only if $\sum_{i=0}^{n-1} c_i \prod_{j\neq i}\left(z+\alpha^j\right) \cong 0(\operatorname{mod} g(z))$, and then use (i).)

Reference

San Ling and Chaoping Xing. *Coding theory, a first course.* Cambridge University Press, 2004